This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A system for communicating data and protecting rights therein, comprising:

at least one user device which communicates wirelessly and is capable of performing a mutual authentication with a server for receiving data;

~~a~~ said server in communication with said at least one user device and including a trusted lock;

a rights management engine in communication with said server for applying and enforcing user rights associated with said data;

a first storage device in communication with said server for storing said data; and

a second storage device in communication with said server for recording a time stamped and digitally signed audit trail;

wherein said server, said rights management engine, said first storage device for storing said data and said second storage device for recording a time stamped and digitally signed audit trail are separate from said at least one user device, and wherein said data is rendered by said server.

Claim 2 (currently amended): The system according to claim 1, wherein said server, said rights management engine, ~~data~~ said first storage device and ~~audit trail~~said second storage device are in a secure location separate from the user device so that trusted services including timing, auditing and copying are performed in a secure environment.

Claim 3 (currently amended): The system according to claim 1, wherein said user device includes a third storage device for holding data which is released under instructions from said server.

Claim 4 (previously presented): The system according to claim 1, wherein said user device is a wireless communication terminal selected from the group consisting of a mobile station, a WAP-

capable cellular telephone, an extended markup language capable cellular telephone, or a cellular telephone with a processor-based system connected to it.

Claim 5 (previously presented): The system according to claim 4, wherein said wireless terminal is an "always on" device.

Claim 6 (previously presented): A method of communicating data from a server to a wireless user device and protecting rights therein, comprising:

authenticating identification of said server and said user device;

requesting data to be communicated from said server to said user device;

authorizing said data to be communicated based on rights attributed to said user device in a rights management engine separate from said user device;

recording said authorization to provide for billing information and an audit trail separate from said user device;

rendering said data from said server to said user device wirelessly.

Claim 7 (original): The method according to claim 6, wherein said data is communicated to said user device and stored therein and rendered in sections according to instructions communicated from said server.

Claim 8 (canceled)

Claim 9 (previously presented): The method according to claim 6, wherein said wireless user device is an "always on" user device.

Claim 10 (canceled)

Claim 11 (original): The method according to claim 6, wherein said recording step is performed in a storage device to record authorization along with time and other information in order to

provide a trusted audit trail, which is based on trusted time and a trusted third party to sign the recording.

Claim 12 (original): The method according to claim 6, wherein said data is originally stored in a content storage device connected to said server.

Claim 13 (previously presented): A rights secure communication device for wirelessly providing data to a user device comprising:

a server, which is capable of performing a mutual authentication with the user device and rendering said data to said user device;

a data storage device connected to said server for storing said data; and

a digital rights management engine connected to said server for determining rights attributed to authenticated users.

Claim 14 (original): The communication device according to claim 13, further comprising a secure storage device for recording authorization of data communication in a secure audit trail.

Claim 15 (currently amended): The communication device according to claim 13, wherein data is sent from said server to ~~a~~ the user device through a wireless communication system.

Claim 16 (previously presented): The communication device according to claim 15, wherein said wireless communication system is an "always on" connection.

Claims 17-18 (canceled)

Claim 19 (previously presented): A computer program embodied on a computer readable medium and executable by a computer to communicate data having protected rights, the program, when executed, performing the steps of comprising:

communicating wirelessly with a mobile terminal controlled by a user;

determining rights of said user in protected data using a rights management engine;

recording an audit trail of communications with said mobile terminal in a storage device; and

rendering said data and wirelessly communicating said data to said mobile terminal.

Claim 20 (previously presented): A computer program according to claim 19, when executed further performing the step of storing said protected data in a secure location separate from said mobile terminal wherein all operations regarding said protected data are performed in a secure environment.

Claim 21 (previously presented): The system according to claim 1, wherein said data is stored in protected form.

Claim 22 (previously presented): The system according to claim 1, wherein said data rendered by the server is formatted and delivered to said at least one user device for use.